ESF

2019년 4월 25일 목요일 오후 4:01

Blue Team

: The Blue team represents and is comprised of your organization's existing information security and IT administration staff.

* **Red Team**

While part of the purpose of red team exercises is to explore how an organization is vulnerable to digital infiltration by an exteral attacker and remediate those vulnerabilities, another important part of red team exercises is to train organizational staff on how to detect, investigate, and respond to attacks against the organization's information systems.

Red team gains complete dominance of the network. The worst outcome from the perspective of the blue team and indicative that the current information systems configuration add incident response policies need revision and remediation.

<<BLUE TEAM GOALS >>

- Stopping the red team from successfully achieving its goals.

- Early detection and effective response to red team activities.

- Post-exercise report.
this report should detail blue team successes and failures. Indepent of the outcome, this report will asstst in improving the processes the internal teams follow when a real, rather than stmulated, attack occurs.

- Revise the incident response strategy.